HACKTOBERFEST
2016
BSIDES
WASHINGTON D.C.

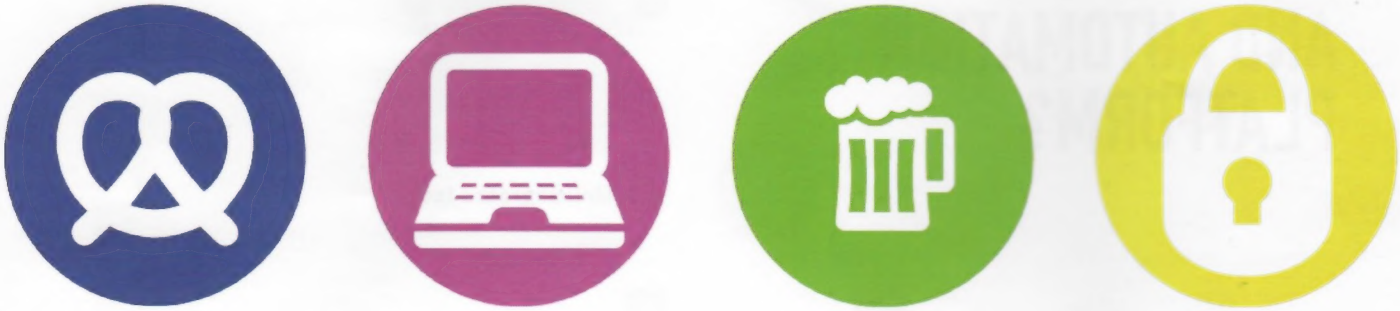
DO YOU NEED A SECURITY ORCHESTRATION AND AUTOMATION PLATFORM?

Visit Komand in the sponsor area
to learn how our security orchestration and automation platform will help you do more, stress less, and respond to threats faster than ever before.

KOMAND
www.komand.com

Welcome to BSides DC!

This year marks our fourth annual event here in Washington DC! This weekend you will experience the culmination of twelve months of hard work by the local members of the information security community to bring you an event worthy of the BSides name. We present to you three days crammed with speakers, training, networking, beer and the very first track for kids! We strive for an open atmosphere of learning, sharing, collaboration, and participation amongst infosec professionals of ALL levels of experience across a wide range of disciplines and backgrounds. So, with no further ado,



Badges

Blue This badge will be issued to all Hacker (Thief) Class Attendees. Rouges! All of them!

Orange If you see this badge, you are in the presence of a Level 42 Wizard of Organization. The holders of this badge are well known for their Charisma, Dexterity with Powerpoint, and melee combat prowess. Should they issue an order, all are expected to obey.

Red Respect the Paladins that are identified by the red badge of security. Their skirmish ability is unparalled and they are especially effective at fighting undead opponents should you find yourself needing back up in that area.

Gold Our Volunteer Scouts should be consulted if you need information or assistance.

White Our speakers wear the White Bard Badge of Knowledge. Be sure to thank them for sharing their knowledge this weekend.

Green Our sponsors are what makes this event possible. These individuals have contributed much to make this event a reality.

Black You probably won't see a black badge. Why? These are the ninjas. They are highly skilled and usually invisible. If you do happen to see one, well, good luck with that.

Press 'nuff said.

Principles & Values

We don't think this should be too complicated. Conduct of all who participate in our community should be based on open dialog, a willingness to learn, and helping each other out. For Security B-Sides DC, our rules of conduct, principles, and values are listed here.

Conduct- We believe that there are simple rules for governance at any meeting of people striving to be a community:

1. Don't be an asshole.
2. Be willing to learn.
3. Be willing to share.
4. Be willing to help.
5. Be willing to listen.
6. Accept criticism.
7. Be kind.

B-Sides DC is not an elementary school. It's not a land full of rainbows and unicorns. Neither is it hell on earth. If you believe someone is misbehaving, acting inappropriately, or acting illegally, start by talking to that person. Confirm your perspective. If you are unable, or unwilling, to do that, that's OK -- find a B-Sides DC Staff member and talk to them.

Principles - Security B-Sides operates under three simple principles:

1. Expand the conversation.
2. Enable people to join the discussion.
3. Get people involved.

B-Sides DC supports those principles as part of our regional B-Sides operation. What that means is that B-Sides DC is **your** conference. It is up to everyone involved to make it happen, to engage in the debates, to speak up and give voice to the issues. Feedback to the organizers is always welcome.

Values - Each B-Sides is a community-driven framework for building events for, and by, information security professionals. The goal is to expand the spectrum of conversation beyond the traditional confines of space and time. B-Sides creates opportunities for individuals to both present and participate in an intimate atmosphere that encourages collaboration. It is an intense event with discussions, demos, and interaction from participants. It is where conversations for the next big thing are happening.

We value

- We lower the barriers for people to participate.
- We involve people in organizing the events, to help them participate, involve a diversity of input, and teach a new generation of organizers.
- We build and use tools that enable greater participation, share ideas, and enable others to share the magic we collectively create. We share our work openly.
- We help grow the community, because a stronger group helps everyone involved.

We participate

- There are no bystanders.
- We all participate in different ways, including: audience, speakers, organizers, sponsors, volunteers.
- We encourage everyone to share their skills, expertise, and talent.

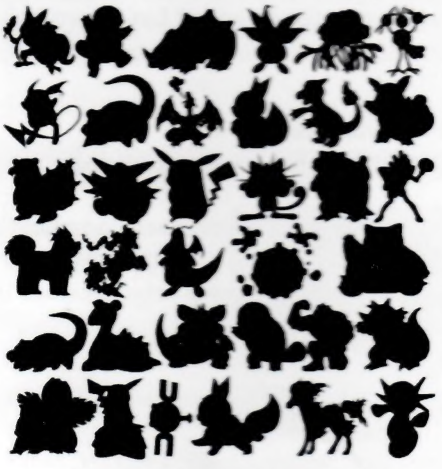
We steward

- We make decisions that strengthen the brand for everyone, not just ourselves.
- We remember that we are not owners of the brand, or the event, but simply caretakers that carry the torch for a period of time, until we pass it to others.
- We treat others with grace and respect at all times.

FRIDAY 21 OCTOBER 2016

	Mount Vernon A Training 1	Mount Vernon B Training 2	Meeting Room 16 Training 3
8:00 AM 9:00 10:00 11:00 12:00 1:00 PM 2:00	**Bro Crash Course** *(Liam Randall)*		**Binary Reverse Engineering for Beginners** *(Benjamin Demick, Michael Schroeder, Malachi Jones, Allen Hazelton)*
3:00 4:00 5:00 6:00 7:00 8:00 9:00	**SANS NetWars Tournament**	**SANS NetWars Tournament**	

CAN YOU CATCH THEM ALL?



/CRYPTODEX

SATURDAY 22 OCTOBER 2016

	Grand South Track 1	Grand Central Track 2	General	Congressional Hall C	Congressional Hall B	Congressional Hall A
8:00 AM						
9:00 AM	**Welcome** *Alex Norman & Bob Weiss* (15 Minutes)	**Welcome** *Alex Norman & Bob Weiss* (15 Minutes)				
9:15 AM	**KEYNOTE** *Marcia Hoffman* (45 Minutes)	**KEYNOTE** *Marcia Hoffman* (45 Minutes)	**BSidesDC** **Registration**		**Wireless Capture the Flag (WCTF)**	**Lockpick Village**
10:00	**Morning Break** (30 Minutes)	**Morning Break** (30 Minutes)	**&**			**&**
10:30	**WCTF Magic as Told by a Clumsy Magician** *Timothy Allmon* (50 Minutes)	**CryptKids Keynote** *Liam Randall* (50 Minutes)	**Storefront**	**2nd Annual BSidesDC CryptKids Con**		**IOT Village**
11:30	**Vulnerability Management Systems Flawed - Leaving Your Enterprise at High Risk** *Gordon MacKay* (50 Minutes)	**Detecting Malicious Websites Using Machine Learning** *Ajit Thyagarajan, Andrew Beard* (50 Minutes)	**Storefront**			
12:30	**LUNCH** *Catered Lunch in the Conference Space Provided by* **ENDGAME** (1 Hour)	**LUNCH** *Catered Lunch in the Conference Space Provided by* **ENDGAME** (1 Hour)				
1:30	**Applying Data Science to Identify Malicious Actors in Enterprise Logs** *Balaji Balakrishnan* (50 Minutes)	**Powershell Security: Defending the Enterprise From the Latest Attack Platform** *Sean Metcalf* (50 Minutes)				
2:30	**Attacking Patient Health: The Anatomy of Hospital Exploitation** *Jacob Holcomb* (50 Minutes)	**Beyond Automated Testing** *Zachary Meyers & Andrew McNicol* (50 Minutes)				
3:30	**Adversarial Post--Exploitation: Lessons From the Pros** *Justin Warner & Chris Ross* (50 Minutes)	**How to Join the Infosec Community** *Micah Hoffman* (50 Minutes)				
4:30	**Act and Think Like an Epidemiologist to Combat Digital Diseases** *Efrain Ortiz* (50 Minutes)	**Abusing Windows With Powershell and Microsoft Debuggers in User-land and Kernel-land** *Pierre-Alexandre Braeken* (50 Minutes)				

SATURDAY 22 OCTOBER 2016 - TRAINING

	Mount Vernon B Training 2	Meeting Room 15 Training 3	Meeting Room 16 Training 4
8:00 AM			
9:00	Cyber Security Exercise CTF presented by Symantec	Building Blocks: The Security Analyst's Toolbox *Kerry Hazelton*	Point 3 Cyber A3 CTF
10:00			
11:00			
12:00			
1:00 PM	0900-1600	0900-1600	0900-1600
2:00			
3:00			
4:00			
5:00			

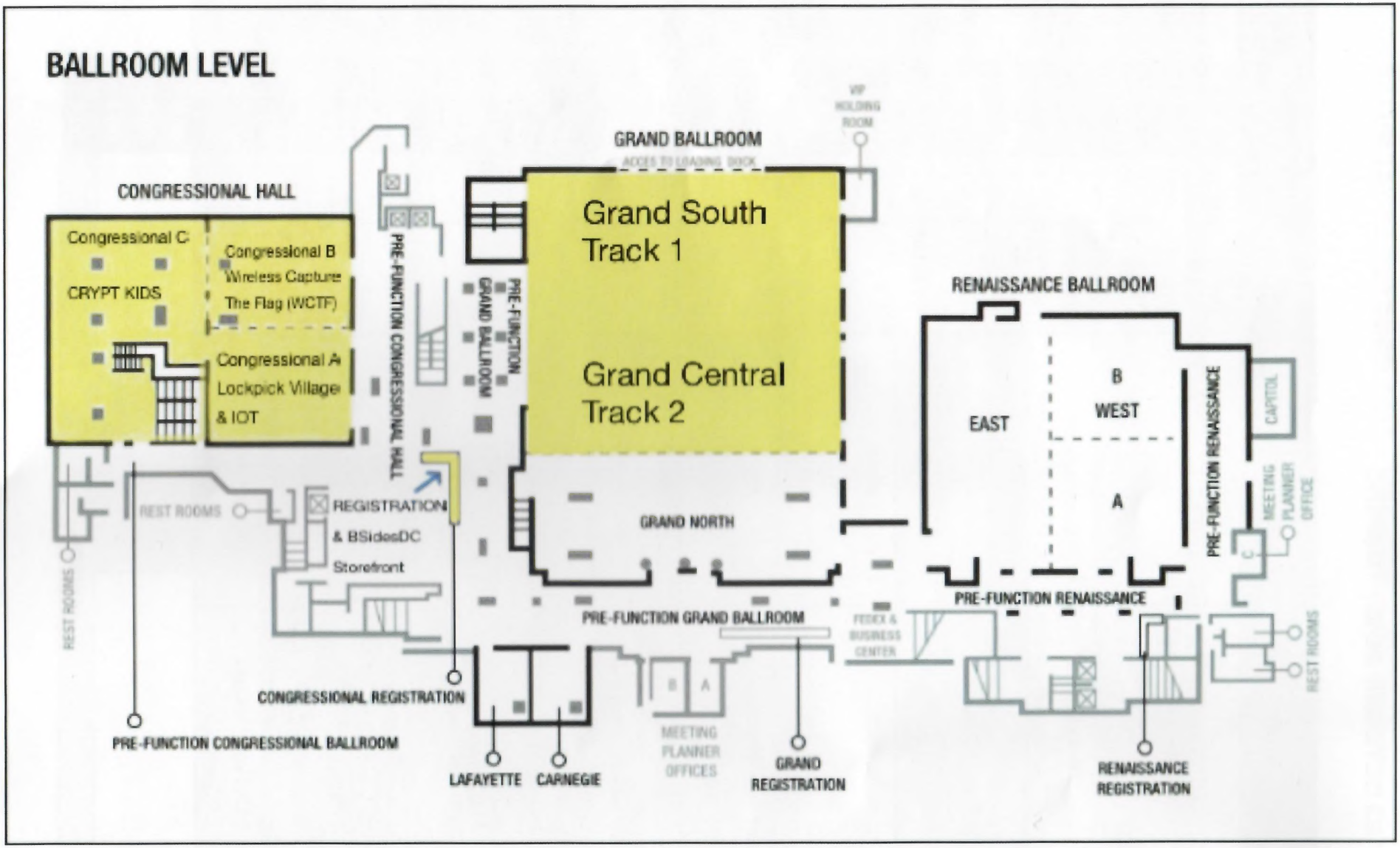
SUNDAY 23 OCTOBER 2016 - TRAINING

	Mount Vernon B Training 2	Meeting Room 15 Training 3	Meeting Room 16 Training 4
8:00 AM			
9:00	Cyber Security Exercise CTF presented by Symantec		Point 3 Cyber A3 CTF
10:00			
11:00			
12:00			
1:00 PM	0900-1600		0900-1600
2:00			
3:00			
4:00			
5:00			

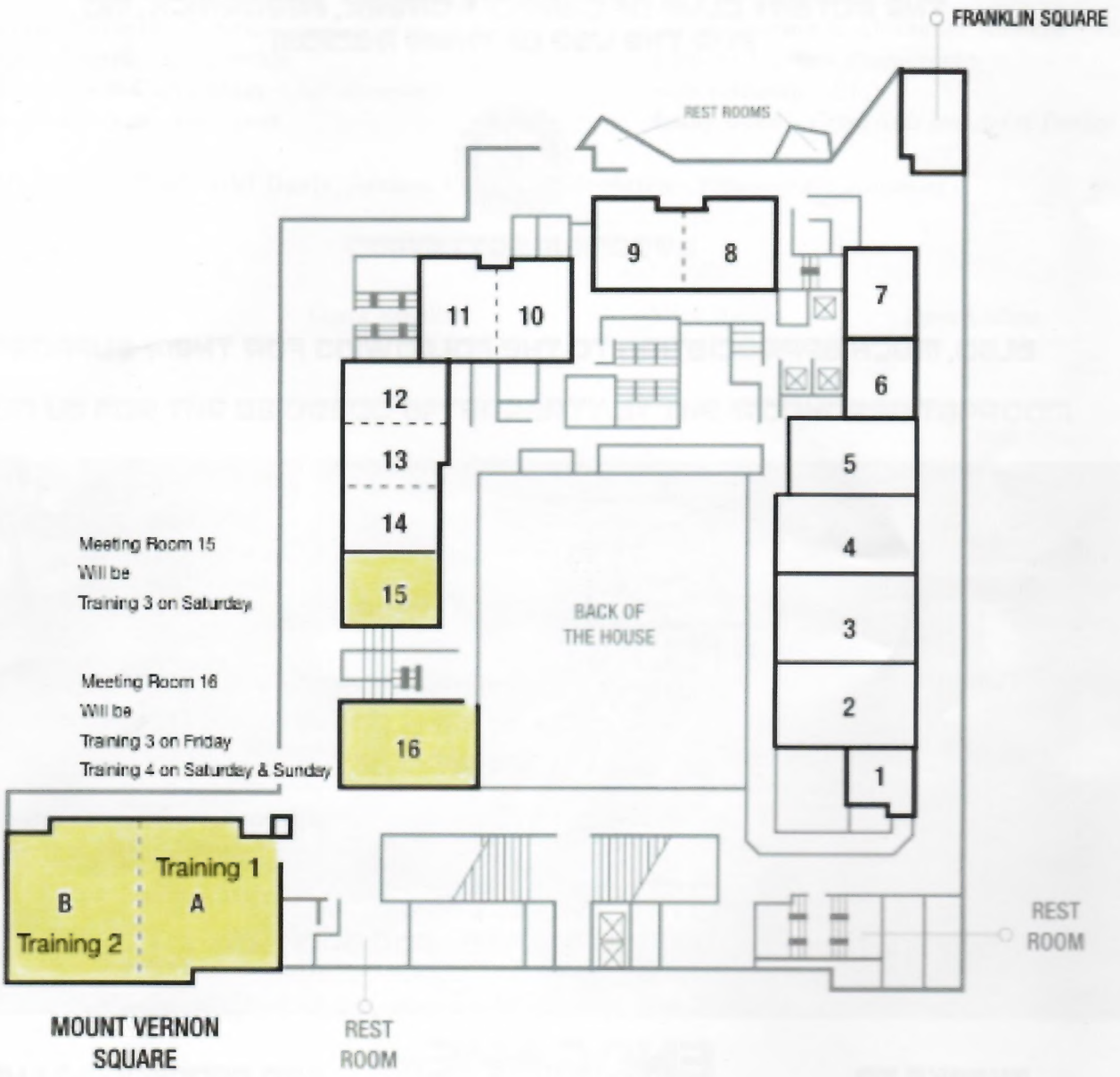
SUNDAY 23 OCTOBER 2016 - TRAINING

	Grand South Track 1	Grand Central Track 2	General	Congressional Hall B	Congressional Hall A
8:00 AM					
9:00	**21st Century War Stories** *Ben Turner* (50 Minutes)	**YAYA (Yet Another Yara Allocution)** *John Laycock & Monty St. John* (50 Minutes)			
10:00	**Morning Break** (30 Minutes)	**Morning Break** (30 Minutes)	**BSidesDC**	**Wireless**	**Lockpick**
10:30	**A Hacker's Guide to Usability Testing** *Greg Norcie* (50 Minutes)	**Cyber Threats and Russian Information and Electronic Warfare** *Paul Joyal* (50 Minutes)	**Registration** **&**	**Capture the Flag (WCTF)**	**Village** **&**
11:30	**LUNCH** (1 Hour)	**LUNCH** (1 Hour)	**Storefront**		**IOT Village**
12:30	**Tales From the Crypt... (Analyst)** *Jeff Man* (50 Minutes)	**Tipping the Scales Back in Our Favour** *Rene Aguero* (50 Minutes)	**Storefront**		
1:30	**"Knowing the Enemy" - Creating a Cyber Threat Actor Attribution Program** *Jack Johnson* (50 Minutes)	**Practical Cyborgism: Getting Started with Machine Learning for Incident Detection** *David Bianco & Chris McCubbin* (50 Minutes)			
2:30	**A Notational Framework for Applying Antifragile Thinking to the RMF-Growing Stronger Through Compromise** *Joe Klein* (50 Minutes)	**Users and Cloud Collide: Understanding Threat Vectors in the Enterprise Cloud Environment** *Ron Zalkind* (50 Minutes)			
3:30	**What's the Big Deal with Assessing ICS/SCADA** *Jim Gilsinn* (50 Minutes)	**Tails of Fails and Tools for Message Integrity** *Jacob Thompson* (50 Minutes)			
4:30	**Closing Remarks** (30 Minutes)	**Closing Remarks** (30 Minutes)			

BALLROOM LEVEL



MEETING ROOM LEVEL



Thank you to Sophos for donating their tech kit to the event!

SOPHOS

Thank you to
The Rotary Club of Carroll Creek, Frederick, MD
for the use of their radios!

Also, much appreciation to the following for their support

Toool DC

VILLAGE

WIRELESS VILLAGE

independent security evaluators

Thanks to antietam TECHNOLOGIES, INC for sponsoring coffee!

Thanks to ENDGAME. for sponsoring lunch.

And a special thank you to all our planning committee members!

Co-Directors

Alex Norman & Robert Weiss

Committee Chairs

Dorann Norman – *Finance*
Angelo Capili – *Sponsorship*
Jim Gilsinn & Corey Sinay – *Infrastructure*
Preston Thomas – *Locksport*
Brett Thorson & Alexander Romero – *Video*
Kellop Charles – *Photography*
Seth Feldman – *CFP*
Jenny Bond – *Crypt Kids and Art & Design*

Nathaniel Davis, Joanne Venema, Forg0tten - *Volunteer Coordinators*

Committee Members

Jim Elliott | Derek Rogillio | Mick Baccio | Dave Cafaro

Join us for the BSidesDC afterparty at the IronHorse Taproom

507 7TH Street NW
Washington, DC 20004
Saturday 22 October 2016
7:00 PM

Sponsored by:

Altus Consulting Corporation

SPONSORS

Events cost money and we desire that very little of these costs be shouldered by the attendees. As with many security BSides, our goal is to provide you with a fantastic, educational, fun filled weekend of information security knowledge sharing and community building at the lowest barrier to entry possible. We give a shout out to our sponsors who have made this event possible for you:

~ENGAGING THE AUDIENCE~

Veris Group ATD Adaptive Threat Division

SANS NETWARS

OMAND

redhat.

~ABOVE AND BEYOND~

COBALTSTRIKE ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

ARUBA networks

ENDGAME.

tenable network security

antietam TECHNOLOGIES, INC

UPLEVEL

ClearedJobs Net

paloalto networks.

ALTUS CONSULTING CORPORATION

FireEye

VENCORE

Symantec.

Point3

VALIANT SOLUTIONS

DEFENSE POINT SECURITY

~ Core Supporters ~

SYSTEM 1, INC.

DISRUPT 6

WarCollar industries

RAPID7

~ Up and Coming ~

Binary Guard

SYNCURITY

KENEXIS

BSIDES WASHINGTON D.C.

Thank you for coming! See you next year!

info@bsidesdc.org
sponsor@bsidesdc.org

BSidesDC

@BSidesDC